

UNITED STATES DISTRICT COURT

for the  
Northern District of Texas

In the Matter of the Search of  
(Briefly describe the property to be searched  
or identify the person by name and address)

Residential property located at 9127 Rainland Court,  
Arlington, Texas, 76002

U.S. DISTRICT COURT  
NORTHERN DISTRICT OF TEXAS  
FILED  
FEB - 9 2017  
CLERK, U.S. DISTRICT COURT  
Case No. 4:17-MJ-145

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A

located in the Northern District of Texas, there is now concealed (identify the person or describe the property to be seized):

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

Offense Description

18 U.S.C. §§ 2252 & 2252A Distribution, receipt, and possession of child pornography.

The application is based on these facts:

See attached Affidavit

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Sworn to before me and signed in my presence.

Date:

2/9/17

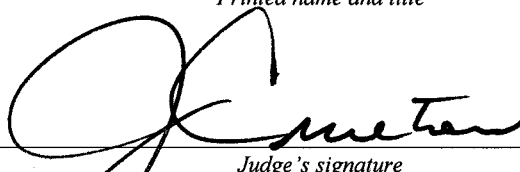
City and state: Fort Worth, Texas



Applicant's signature

LeAndrew J. Mitchell, Special Agent

Printed name and title



Judge's signature

Jeffrey L. Cureton, U.S. Magistrate Judge

Printed name and title

**AFFIDAVIT IN SUPPORT OF SEARCH WARRANT APPLICATION**

I, LeAndrew J. Mitchell, being duly sworn under oath, do hereby depose and state:

1. I am a Special Agent with the United States Department of Homeland Security, Homeland Security Investigations (HSI), and I have been employed in this capacity since December 2008. I am a graduate of the Criminal Investigator Training Program and the U.S. Immigration and Customs Enforcement Special Agent Training Academy. As a result of my employment with HSI, my duties include, but are not limited to, the investigation and enforcement of Titles 8, 18, 19, 21 and 31 of the United States Code (U.S.C.). I am an “investigative or law enforcement officer of the United States” within the meaning defined in 18 U.S.C. § 2510(7), in that I am an agent of the United States authorized by law to conduct investigations of, and make arrests for, federal offenses.

2. As part of my duties as an HSI agent, I investigate criminal violations relating to the sexual exploitation of children, including the illegal production, distribution, receipt, and possession of child pornography, in violation of 18 U.S.C. §§ 2251, 2252 and 2252A. I have received training in the areas of child pornography and child exploitation, and have observed numerous examples of child pornography, as defined in 18 U.S.C. § 2256, in all forms of media. I have been involved in several child exploitation investigations, and I am familiar with the tactics used by offenders who collect and distribute child pornographic material.

3. This affidavit is made in support of an application for a warrant authorizing the search of the residential property at **9127 Rainland Court, Arlington, Texas, 76002**, located within the Northern District of Texas, and further described in Attachment A incorporated with this affidavit. I seek authorization to search the entire residential premises and any computers and electronic media therein, for the items specified in Attachment B, which constitute evidence and instrumentalities of violations of 18 U.S.C. §§ 2252 and 2252A (distribution, receipt, and possession of child pornography).

4. The information set forth in this affidavit comes from an investigation I have conducted, my training and experience, and information obtained from other law enforcement officers. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have only set forth those facts that I believe are necessary to establish probable cause to believe that evidence, fruits and/or instrumentalities of violations of 18 U.S.C. §§ 2252 and 2252A are presently located at **9127 Rainland Court, Arlington, Texas**.

#### **DEFINITIONS**

5. The following definitions, inclusive of all definitions contained in 18 U.S.C. § 2256, apply to this affidavit and Attachment B incorporated herein:

a. “Child Erotica” means materials or items that are sexually arousing to persons who have a sexual interest in minors, but that are not necessarily obscene, or that do not necessarily depict minors in sexually explicit poses or positions.

b. “Computer” refers to any electronic, magnetic, optical, electrochemical, or other high speed data processing device capable of performing logical or storage functions, and includes any data storage facility or communications facility directly related to such a device. As used herein, “computer” also incorporates digital devices that complete these same functions, such as smartphones, tablets, connected devices, and e-readers. See 18 U.S.C. § 1030(e)(1).

c. “Computer hardware” consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

d. “Computer passwords and data security devices” consist of information or items designed to restrict access to computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates what might be termed a digital key to “unlock” particular data security devices. Data security hardware may include encryption devices, chips, and/or circuit boards. Data security software of digital

code may include programming code that creates “test” keys or “hot” keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or “booby-trap” protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

e. “Computer software” is digital information that can be interpreted by a computer and any of its related components to direct the way it works. It commonly includes programs to run operating systems, applications, and utilities.

f. “Internet Protocol address” or “IP address” refers to a unique number used by a computer to access the Internet. IP addresses can be dynamic, meaning that the Internet Service Provider (ISP) assigns a different unique number to a computer every time it accesses the Internet. IP addresses may also be static, which means the ISP assigns a user’s computer a particular IP address that is used each time the computer accesses the Internet.

g. “Cloud-storage service” refers to a publicly accessible, online storage provider that can be used to store and share files in large volumes. Users of cloud-storage services can share links and associated passwords to their stored files with others in order to grant access to their file collections. Such services allow individuals to easily access these files through a wide variety of electronic devices such as desktop computers, laptops, mobile phones or tablets, from anywhere. Many services provide free access up to a certain size limit.

h. “Electronic Mail,” commonly referred to as e-mail (or email), is a method of exchanging digital messages from an author to one or more recipients. Modern email

operates across the Internet or other computer networks. Email systems are based on a store-and-forward model; that is, email servers accept, forward, deliver, and store messages. Neither the users nor their computers are required to be online simultaneously; they need only connect briefly, typically to an email server, for as long a period of time as it takes to send or receive messages. An Internet email message generally consists of three components: the message envelope, the message header, and the message body; in some cases, it may include a fourth component, an attachment. Email attachments can include any type of digital file. There are numerous methods of obtaining an email account; some of these include email accounts issued by an employer or an education authority. One of the most common methods of obtaining an email account is through a free web-based email provider such as Microsoft, Yahoo!, or Google. Anyone with access to the Internet can generally obtain a free web-based email account.

i. “Communication channel” means a medium through which a message can be transmitted to its intended audience, such as a print media or electronic media (e.g., oral communications or broadcast). In account subscriptions, it refers to a means of delivering account information to a customer, like email, telephone communication, or facsimile.

j. The terms “records,” “documents,” and “materials,” as used herein, include all information recorded in any form, both visually or aurally, and by any means, whether in handmade form (e.g., writings, drawings, and paintings), photographic form (e.g., microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, and photocopies), mechanical form (e.g., phonograph records, printing, or typing), or

electrical, electronic, or magnetic form (e.g., tape recordings, cassettes, compact discs, electronic, or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks or DVDs, Personal Digital Assistants (PDAs), Multimedia Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

### **BACKGROUND ON COMPUTERS AND CHILD PORNOGRAPHY**

6. Based on my training and experience in child exploitation investigations, I am aware that computers, computer technology and the Internet significantly facilitate the distribution, receipt and possession of child pornography. Child pornography offenders can transpose photographic images from a camera into a computer-readable format with a scanner. With digital cameras, smartphones or tablets, the images can be transferred directly onto a computer. A modem allows any computer to connect to another computer through the use of a telephone, cable, or wireless connection. Therefore, through use of the Internet, electronic contact can be made with literally millions of computers around the world.

7. A computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown significantly within the last several years. These drives can store thousands of images at very high resolution. Additionally, electronic devices such as smartphones (e.g., Apple iPhones), connected devices (e.g., Apple iTouch), e-readers, and tablets (e.g., Apple iPads, Kindle

Fire) now function essentially as computers with the same abilities to store images in digital form.

8. The Internet affords collectors of child pornography several different venues for obtaining, viewing and trading child pornography in a relatively secure and anonymous fashion. Collectors and distributors of child pornography also use online resources to retrieve and store child pornography, including, but not limited to, services offered by Internet portals such as Gmail and Outlook. These online services allow a user to set up an account with a remote computing service that provides email services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer or device with access to the Internet, and evidence of such online storage of child pornography is often found on the user's computer or device.

9. Even when files on a computer have been deleted, they can be recovered months or years later using readily available forensic tools. When an individual deletes a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside on the hard drive in space that is not allocated to an active file for long periods of time before they are overwritten.

10. A computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Additionally, files that have been viewed on the Internet are automatically downloaded into a temporary Internet directory or "cache." Browsers typically maintain a fixed amount of hard drive space devoted to these files, and the files



are only overwritten as they are replaced with more recently viewed Internet pages.

Therefore, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed, and more on the user's operating system, storage capacity, and computer habits.

### **SPECIFICS REGARDING THE SEARCH AND SEIZURE OF COMPUTERS**

11. Based on my training and experience, I am aware that the search of computers often requires agents to seize most of the computer items (e.g., hardware, software and instructions) to be processed later by a qualified computer expert in a laboratory or other controlled environment. That is essential to the search for electronic evidence because of the following facts:

a. Computer storage devices, like hard drives, diskettes, tapes, or laser disks, store the equivalent of thousands of pages of information. When a user wants to conceal electronic evidence of a crime, he or she may store it in random order with deceptive file names. This requires searching authorities to examine all of the stored data to determine whether it is included within the scope of the warrant. This process can take weeks or months, depending on the volume of the stored data, and it would be impractical to attempt this kind of data search on-site;

b. Searching computer systems for criminal evidence is a highly technical process that requires advanced training and a properly controlled environment. The vast array of computer hardware and software available today requires even computer experts to specialize in specific systems and applications. It is difficult to know prior to a search which expert should analyze the system and its data. The search of a computer system

can be equated to a scientific procedure, which is designed to protect the integrity of the evidence while recovering hidden, erased, compressed, password-protected, and other encrypted files. Because computer evidence is extremely vulnerable to tampering and destruction, both from external sources and from code embedded in the system as a “booby-trap,” the controlled environment of a laboratory is essential to its complete and accurate analysis;

c. In order to fully retrieve data from a computer system, an analyst needs all magnetic storage devices, as well as the central processing unit (CPU). For child pornography investigations, in which the evidence consists partly of graphic files, the monitor and printer are also essential to show the nature and quality of the graphic images that the system can produce. The analyst needs all assisting software (e.g., operating systems or interfaces, and hardware drivers) and any applications software, which may have been used to create the data, as well as all related instructional manuals, documentation and security devices;

d. Searching computerized information for evidence or instrumentalities of a crime often requires the seizure of the entire computer’s input/output periphery devices, including related documentation, passwords and security devices, so that a qualified examiner can accurately retrieve the system’s data in a controlled environment. Peripheral devices, which allow users to enter and retrieve data from stored devices, vary widely in their compatibility with other hardware and software. Many system storage devices require particular input/output devices in order to read the data on the system; therefore, it is important that the analyst be able to properly retrieve the evidence sought.

12. The facts set forth in this affidavit establish probable cause to believe that a computer, its storage devices, and other system components were used as a means of committing offenses involving the sexual exploitation of children, in addition to storing evidence of said crime. Accordingly, I seek the authorization to seize and search any computers and related electronic devices located at **9127 Rainland Court, Arlington, Texas**, consistent with the scope of the requested search.

### **OVERVIEW OF INVESTIGATION**

13. In March 2016, the New Zealand Department of Internal Affairs (NZDIA) conducted an online investigation into several accounts hosted by Mega Limited (hereinafter, "Mega"), which is a cloud-storage, file-hosting website headquartered in New Zealand. As a result of this investigation, the NZDIA identified a particular Uniform Resource Locator (URL) that contained over 100 files of child exploitative material.

14. The NZDIA subsequently obtained the contents of the account associated with this URL pursuant to New Zealand law, which included the subscriber and log-in records associated with the account. The records obtained for the account included the following subscriber information:

Account user ID: 10106092550  
Registered Email Address: fakespamemail908@gmail.com  
Account Creation Date: July 3, 2015  
IP Addresses: 70.116.154.161; 173.173.90.244

15. NZDIA personnel conducted research into the IP addresses used to create and access this Mega account, and learned both IP addresses are owned by Time Warner

Cable and resolve to the Arlington, Texas area. Since the user of this account appeared to reside in the United States, the NZDIA routed the information through Interpol to the HSI Cyber Crimes Center (C3) in Fairfax, Virginia.

16. On or about November 8, 2016, HSI C3 served a subpoena on Time Warner Cable for the subscriber assigned IP address 173.173.90.244 on July 7, 2016, which was the last access date provided in the Mega subscriber records. On or about November 16, 2016, Time Warner Cable complied with the subpoena, and provided the following subscriber information:

Subscriber Name: Steven Bell  
Subscriber Address: **9127 Rainland Court, Arlington, Texas**  
Account Deactivation Date: September 9, 2016

17. On or about November 18, 2016, HSI C3 forwarded this case to the HSI Dallas Child Exploitation Group, and your affiant was assigned the investigation. On or about December 5, 2016, I obtained a copy of the contents stored in the Mega account under investigation, and observed numerous files that depicted child pornography. The following provides an example of the files that were stored in the Mega account associated with fakespamemail908@gmail.com:

File Name	Description
10Yo 10Yr Kinderfickervideo Pedoland Papa Vater Fickt (Kinder)-1.avi	A two minute, two second video of a nude prepubescent female child who is bound by the ankles. During the video, an adult male has vaginal and anal intercourse with the child.

000262.mp4	A fifty-four second video of a nude prepubescent male child. During the video, the child inserts an object into his anus while lasciviously displaying his genitals.
0525.mp4	A forty-one second video of a prepubescent male child performing oral sex on an adult male.

Based on my training and experience in child exploitation investigations, I submit that these files constitute child pornography, as defined in 18 U.S.C. § 2256.

18. On or about December 5, 2016, HSI Dallas served a subpoena on Google for the subscriber information relating to fakespamemail908@gmail.com. On or about December 15, 2016, Google complied with the subpoena by providing the following subscriber information for this account:

Name: Spam Spammy  
Recovery Email: gemini908@gmail.com  
SMS: 817-897-[redacted]

19. On December 27, 2016, HSI Dallas obtained search warrants from United States Magistrate Judge Hal R. Ray, Jr., authorizing the search of Google accounts fakespamemail908@gmail.com and gemini908@gmail.com. The warrants were served on Google on this same date. On or about January 17, 2017, and January 20, 2017, Google provided the contents of fakespamemail908@gmail.com and gemini908@gmail.com, respectively.

20. On or about January 25, 2017, I began reviewing the contents of these Google accounts. The search of fakespamemail908@gmail.com revealed several email communications regarding the distribution of child pornography by the user of this

account. There were multiple messages in which the user of this account distributed the URL of the Mega cloud-storage account containing child pornography that prompted this investigation. Certain email messages in the account indicate the user has been communicating with individuals through a particular website (hereinafter, "Website A"), which is known to law enforcement to be a meeting place for individuals interested in trading child pornography. The following is an example of an email stored in this account:

Message From: fakespamemail908@gmail.com  
 Message To: [redacted]@outlook.it  
 Subject: "[Website A]"  
 Sent: July 7, 2015 at 3:50 p.m.  
 Message Body: "Hey. I saw your post on [Website A]. I have a link to 110+ vids. would you want to trade?"

21. The search of the gemini908@gmail.com account revealed several personal email messages to and from Jordan Lee Bell, who has been identified as the probable suspect responsible for the accounts under investigation. The account also contained over 130 video files depicting child pornography, to include videos and images of prepubescent children. These files were located in various folders, including, but not limited to folders labelled "13yo," "14yo," "youngset1" and "youngset2." The following provides an example of the files that were stored in Google account gemini908@gmail.com:

File Name	Description
5 (2).mp4	A fifty-three second video of a prepubescent male child who is approximately 9 to 11 years old. During the video, an individual touches the child's penis as the child ties a rope around his ankle.

04.avi	A one minute, eighteen second video of a prepubescent female minor who is asleep. During the video, an adult male masturbates and ejaculates on the child's face.
0525.mp4	A forty-one second video of a prepubescent male child who is approximately 5 to 7 years old. During the video, the child performs oral sex on an adult male.

Based on my training and experience in child exploitation investigations, I submit that these files constitute child pornography, as defined in 18 U.S.C. § 2256.

22. The records provided by Google included any available metadata associated with the image and video files uploaded to the gemini908@gmail.com account. A review of this metadata indicates there were images uploaded to the account that were captured by an iPhone 4s and an Asus Nexus 7 tablet. There were also several messages sent from this account that contained an email signature that read "Sent from my iPhone."

23. The Google search warrant records also included log-in session data, which indicates the gemini908@gmail.com account was accessed on December 24, 2016, using IP address 2605:6000:151e:c002:489c:cb10:515a:835b, and on December 26, 2016, using IP address 2605:6000:151e:c002:a57c:f7c3:3a9f:a65f. On January 30, 2017, HSI Dallas served a subpoena on Time Warner Cable for the subscriber information relating to the customer assigned these IP addresses on the dates that they were used to access gemini908@gmail.com. On February 1, 2017, Time Warner Cable reported that both IP addresses were assigned to the following customer at the times they were used to access this Google account:

Subscriber Name: Steven Bell  
Subscriber Address: **9127 Rainland Court, Arlington, Texas**  
Activate Date: September 12, 2016

24. On February 3, 2017, I conducted surveillance at **9127 Rainland Court, Arlington, Texas**. At approximately 6:47 a.m., I observed Jordan Bell leave the residence and depart in a black Toyota Camry displaying Texas license plate [redacted], which was parked in the cul-de-sac in front of the residence. Texas motor vehicle records indicate this vehicle is registered to Steven and Patricia Bell, **9127 Rainland Court, Arlington, Texas**. I was able to positively identify Jordan Bell from a copy of his Texas driver's license, which also lists **9127 Rainland Court, Arlington, Texas** as his current address.

25. Tarrant County Central Appraisal District (CAD) records indicate **9127 Rainland Court, Arlington, Texas** is owned by Steven and Patricia Bell. The Consolidated Lead Evaluation Reporting (CLEAR) public records database also indicates this address is associated with the Bell family, whose members include Steven Bell, Patricia Bell, Jordan Bell, M. Garcia, and S. Garcia.

#### **CHARACTERISTICS OF CHILD PORNOGRAPHY COLLECTORS**

26. I respectfully submit that the information set forth in this affidavit establishes probable cause to believe that an individual using the Internet services at **9127 Rainland Court, Arlington, Texas** has distributed and possessed child pornography, or has attempted to commit said crimes. Based on training, experience, and numerous interviews with subjects who admitted to having a sexual interest in children, I am aware



that the following characteristics are common to individuals involved in child pornography offenses:

a. Individuals who possess, receive, or distribute child pornography may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity, sexually suggestive poses, or from literature describing such activity;

b. Individuals who possess, receive, or distribute child pornography may collect sexually explicit or sexually suggestive material depicting children, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. These individuals often maintain this material for sexual arousal and gratification. Furthermore, they may use this material to lower the inhibitions of children they are attempting to seduce, to arouse a child partner, or to demonstrate the desired sexual acts;

c. Individuals who possess, receive, or distribute child pornography often possess and maintain copies of child pornographic material, including but not limited to pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, and tape recordings, in the privacy and security of their home. Prior investigations into these offenses have shown that child pornography offenders typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years;

d. Individuals who possess, receive, or distribute child pornography often begin their child pornography collections by obtaining child abuse material through

various free avenues afforded by the Internet. Thereafter, these individuals may escalate their activities by producing and/or distributing child pornography, for the purpose of trading this material to add to their own child pornography collection;

e. Individuals who possess, receive, or distribute child pornography often maintain their digital or electronic collections in a safe, secure and private environment, such as a computer or surrounding area. These collections are often maintained for several years and are maintained at the individual's residence or place of employment, to afford immediate access to view the material;

f. Individuals who possess, receive, or distribute child pornography may correspond with others to share information and material, and rarely destroy this correspondence. These individuals often maintain lists of names, email addresses and telephone numbers of others with whom they have been in contact regarding their shared interests in child pornography.

27. The facts set forth in this affidavit indicate that the individual using Google accounts fakespamemail908@gmail.com and gemini908@gmail.com meets the characteristics of a collector of child pornography because: 1) the user has maintained a child pornography collection using multiple Internet platforms, including Mega cloud-storage and Gmail accounts; and 2) the user has corresponded with other individuals regarding the distribution and receipt of child pornography, and has saved this correspondence for an extended period of time. Such activity indicates a user of the Internet services at **9127 Rainland Court, Arlington, Texas** fits the characteristics of a collector of child pornography.

**BIOMETRIC AUTHENTICATION ON DIGITAL DEVICES**

28. Based on the facts set forth in this affidavit, and more specifically the information referenced in Paragraph 22, I believe that the premises to be searched will contain mobile electronic devices such as smartphones, tablets and e-readers, which will contain evidence subject to search and seizure under this warrant. Based on my training, experience, and publicly available information, I am aware that Apple, Motorola, and Samsung, as well as other companies, produce digital devices that can be unlocked via the use of a fingerprint or thumbprint in lieu of a numeric or alphanumeric passcode or password. Each company has a different name for this biometric authentication feature; for example, Apple's version is called "Touch ID."

29. If a user enables the Touch ID feature on an Apple device, he or she can register up to five fingerprints that can be used to unlock that device. The user can then use any of the registered fingerprints to unlock the device by pressing the relevant finger(s) to the device's Touch ID sensor, which is found in the round button (often referred to as the "home button") at the bottom of the device. Based on my training and experience, I am aware that users of Touch ID-capable devices often utilize this feature because it is a more convenient way to unlock the device, as well as a more secure way to protect the device's contents. This is particularly true when the user of the device is engaged in criminal activity, and has a heightened concern about securing the contents of the device.

30. In some circumstances, a fingerprint cannot be used to unlock a Touch ID-enabled device, and a passcode or password must be used instead. These circumstances

include: 1) when more than 48 hours have passed since the device has been unlocked; 2) when the device has been turned on or restarted; 3) when the device has received a remote lock command; or 4) after five attempts to match a fingerprint have been unsuccessful. Other brands have similar restrictions for their biometric authentication features.

31. The passcode or password that may be needed to unlock the digital device(s) found during the search of **9127 Rainland Court, Arlington, Texas** is not known to law enforcement. Thus, it will likely be necessary to use the fingerprints or thumbprints of the user(s) of any fingerprint sensor-enabled device(s) found during the search, in order to unlock the device(s) for the purpose of searching for the evidence subject to seizure under this warrant.

32. Therefore, I request the authority to compel the use of the fingerprint(s) or thumbprint(s) of any person who is located at **9127 Rainland Court, Arlington, Texas** during the execution of the search, who is reasonably believed by law enforcement to be the user of a fingerprint sensor-enabled device located at this residence. The requested authorization is necessary because the Government may not otherwise be able to access the data contained on these devices for the purpose of searching for the evidence subject to seizure under this warrant.

### **CONCLUSION**

33. Based on the information set forth in this affidavit, there is probable cause to believe that evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 2252 and 2252A are present at **9127 Rainland Court, Arlington, Texas**, and the digital media

therein. Accordingly, I request that this Court authorize the search of this residence, including any vehicles located at or near the premises that fall under the dominion and control of the persons associated with said premises, so that agents may seize the items listed in Attachment B.

34. Rule 41 of the Federal Rules of Criminal Procedure authorizes the Government to seize and retain evidence and instrumentalities of a crime for a reasonable time to examine, analyze, and test them. I further request that the Court authorize the transfer of any computers, computer storage devices or smartphones to other Government-authorized personnel or contractors, within or outside of this District, in the event that advanced expertise is needed to access the files subject to search and seizure under this warrant.

  
LeAndrew J. Mitchell, Special Agent  
Homeland Security Investigations

Subscribed and sworn to before me this 9<sup>th</sup> day of February, 2017.

  
JEFFREY L. CURETON  
UNITED STATES MAGISTRATE JUDGE

**ATTACHMENT A**

**DESCRIPTION OF LOCATION TO BE SEARCHED**

9127 Rainland Court, Arlington, Texas 76002

The property to be searched is described as two-story, single family residence constructed of brick and siding. There is an attached garage in the front of the residence, and the number “9127” is displayed within the brick to the left of the garage door. The residence is located in Arlington, Tarrant County, Texas, which is within the Northern District of Texas. The search warrant includes any vehicles located at or near the premises, which fall under the dominion and control of any person(s) associated with said premises. The search of these vehicles is to include all internal and external compartments or containers, which may reasonably store child pornographic materials or their instrumentalities.



**ATTACHMENT B**

**DESCRIPTION OF ITEMS TO BE SEIZED AND SEARCHED**

1. Computers, tablets, computer hardware, computer software, computer related documentation, computer passwords and data security devices, cellular devices, video recording devices, video recording players, videotapes and video display monitors that may be, or are used to do the following: visually depict child pornography or child erotica; display or access information pertaining to a sexual interest in child pornography; display or access information pertaining to sexual activity with children; or distribute, possess, or receive child pornography, child erotica, or information pertaining to an interest in child pornography or child erotica.
2. Evidence of who used, owned, or controlled the computers and cellular devices at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and Internet Service Provider accounts/records.
3. Records evidencing occupancy or ownership of the premises described above, including, but not limited to, utility and telephone bills, mail envelopes, or addressed correspondence, rental or lease agreements, mortgage documents, rental or lease payments and credit card information, including, but not limited to, bills and payment records.
4. Any and all notes, documents, records, computer files or correspondence, in any format and medium (including, but not limited to, envelopes, letters, papers, e-mail

messages, chat logs and electronic messages, and handwritten notes) pertaining to the production, possession, receipt, or distribution of child pornography as defined in 18 U.S.C. § 2256(8), or to the production, possession, receipt, or distribution of visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2).

5. Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) that concern online storage or other remote computer storage, including, but not limited to, software used to access such online storage or remote computer storage, user logs or archived data that show connection to such online storage or remote computer storage, and user logins and passwords for such online storage or remote computer storage.

6. Any and all cameras, film, videotapes or other photographic equipment.

7. During the execution of this search warrant, law enforcement personnel are authorized to press the fingerprints and/or thumbprints of any person located at the residence during the execution of this warrant, to the fingerprint sensor of any device reasonably believed by law enforcement to be used by the person, for the purpose of attempting to unlock the device in order to search the contents as authorized by this warrant.